L Number	Hits	Search Text	DB	Time stamp

-	98	("5659767" "5906397" "6694053" "6044375" "5784487" "6115482" "5903904" "5987171" "6014458" "4891750" "5237627" "5445369" "5475505" "5848186" "5973710" "6082619" "6163623" "6226658" "6226658" "5764799" "4876730" "4941189" "5642473" "4247907" "5247591" "5528732" "5579407" "5848184" "6050490" "6072907" "6400845" "6251576" "6067559" "6330689" "6158779" "5555362" "6003033" "4617410" "5818976" "6064778" "6094665" "6567628" "4394092" "6094484" "4804949" "5199084" "5301243" "5517586" "5805747" "5888367").pn. ("6036094" "6055530" "6086738" "6138129" "6178417" "6201901" "6418244" "6419150" "5212229" "6403337" "6391536" "6468726" "5977972" "6017117" "6135586" "6227660" "5590260" "5801698" "5897644" "5956736" "6216157" "6216157" "6303282" "6423485" "5359412" "5359207"	USPAT	2004/08/13 14:57

-	1	(("5659767" "5906397" "6694053" "6044375" "5784487" "6115482" "5903904" "5987171" "6014458" "4891750" "5237627" "5445369" "5475505" "5848186" "5973710" "6082619" "6163623" "6226658" "6226658" "5764799" "4876730" "4941189" "5642473" "4247907" "5247591" "5528732" "5579407" "5848184" "6050490" "6072907" "6400845" "6251576" "6067559" "6330689" "6158779" "5555362" "6003033" "4617410" "5818976" "6064778" "6094665" "6567628" "4394092" "6094484" "4804949" "5199084" "5301243" "5517586" "5805747" "5888367").pn. ("6036094" "6055530" "6086738" "6138129" "6178417" "6201901" "6418244" "6419150" "5212229" "6403337" "6391536" "6468726" "5977972" "6017117" "6135586" "6227660" "5590260" "5801698" "5897644" "5956736" "6216157" "6216157" "6203282" "6423485" "5399412" "5359207"	USPAT	2004/08/13 14:58

-	0	(("5659767" "5906397" "6694053" "6044375" "5784487" "6115482" "5903904" "5987171" "6014458" "4891750" "5237627" "5445369" "5475505" "5848186" "5973710" "6082619" "6163623" "6226658" "6226658" "5764799" "4876730" "4941189" "5642473" "4247907" "5247591" "5528732" "5579407" "5848184" "6050490" "6072907" "6400845" "6251576" "6067559" "6330689" "6158779" "5555362" "6003033" "4617410" "5818976" "6064778" "6094665" "6567628" "4394092" "6094484" "4804949" "5199084" "5301243" "5517586" "5805747" "5888367").pn. ("6036094" "6055530" "6086738" "6138129" "6178417" "6201901" "6418244" "6419150" "5212229" "6403337" "6391536" "6468726" "5977972" "6017117" "6135586" "6227660" "5590260" "5801698" "5897644" "5956736" "6216157" "6216157" "6303282" "6423485" "5359412" "5359207"	USPAT	2004/08/13 15:00

-	1113	(send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)	USPAT	2004/08/13 15:02
-	7393	380/$.ccls.	USPAT	2004/08/13 15:02
-	328	((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.	USPAT	2004/08/13 15:02
-	249	(((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)	USPAT	2004/08/13 15:03
-	246	((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116	USPAT	2004/08/13 15:05
-	246	(((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116)	USPAT	2004/08/13 15:06
-	246	(((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116) and ((data or message) with (seed or random near3 number))	USPAT	2004/08/13 15:08
-	246	(((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116) and ((data or message) same (seed or random near3 number))	USPAT	2004/08/13 15:08
-	192	(((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116) and ((data or message) near4 (seed or random near3 number))	USPAT	2004/08/13 15:09
-	0	((((((send or sent or transmit$4 or transfer$6) with (seed or (random near3 number)) with (message or data or packet)) and 380/$.ccls.) and key$1 with (seed or random adj number)) and @ad<20010116) and ((data or message) near4 (seed or random near3 number))) and ("security parameter index" or "encapsulating security payload" or ESP)	USPAT	2004/08/13 15:11
-	3912	"security parameter index" or "encapsulating security payload" or ESP	USPAT	2004/08/13 15:11
-	504886	"security parameter index" or "encapsulating security payload" or ESP	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:12
-	396	("security parameter index" or "encapsulating security payload" or ESP) and data adj packet$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:12
-	47	(("security parameter index" or "encapsulating security payload" or ESP) and data adj packet$1) and (seed or random near4 (number or generator))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:19

-	21	((("security parameter index" or "encapsulating security payload" or ESP) and data adj packet$1) and (seed or random near4 (number or generator))) and @ad<20010101	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:17
-	1	((((("security parameter index" or "encapsulating security payload" or ESP) and data adj packet$1) and (seed or random near4 (number or generator))) and @ad<20010101) and 380/$.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:17
-	19789	((key or seed) with message)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:20
-	3303	(send or sent or transmi$6) near5 ((key or seed) with message)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:21
-	788	((send or sent or transmi$6) near5 ((key or seed) with message)) and (random near3 (number or generator))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:21
-	756	(((send or sent or transmi$6) near5 ((key or seed) with message)) and (random near3 (number or generator))) and (encrypt$5 or decrypt$5 or enciph$6 or deciph$5 or encod$6 or decod$6)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:22
-	457	((((send or sent or transmi$6) near5 ((key or seed) with message)) and (random near3 (number or generator))) and (encrypt$5 or decrypt$5 or enciph$6 or deciph$5 or encod$6 or decod$6)) and @ad<20010101	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:34
-	1967	380/43,284,285,44,277,278,279,283.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:38
-	444	("security parameter index" or "encapsulating security payload" or ESP) and (random near3 (number or sequen$6))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:40
-	847	380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequen$6))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:43
-	620	(380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequen$6))) and @ad<20010101	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:41
-	207	((380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequen$6))) and @ad<20010101) and (seed or master near4 key)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:42
-	33	(((380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequen$6))) and @ad<20010101) and (seed or master near4 key)) and wireless	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:42
-	838	380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequence))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:44

-	612	(380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequence))) and @ad<20010101	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:44
-	103	((380/43,284,285,44,277,278,279,283.ccls. and (random near3 (number or sequence))) and @ad<20010101) and wireless	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:46
-	2739	seed with random	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:46
-	490	(seed with random) and 380/$.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:47
-	67	((seed with random) and 380/$.ccls.) and seed with message	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:58
-	39	(((seed with random) and 380/$.ccls.) and seed with message) and @ad<20010101	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:47
-	22	((seed with random) and 380/$.ccls.) and seed with random with key with message	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/13 15:58

Refine Search

Search Results -

Term	Documents
(2 AND 6).USPT.	18
(L6 AND L2).USPT.	18

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L7

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Friday, August 13, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L7	L6 and l2	18	L7
L6	L5 and l4	496	L6
L5	transmission near2 (seed or key)	2326	L5
L4	(encrypted or enciphered or encoded) adj (message or data)	19324	L4
L3	(encrypted or enciphered or encoded) adj (message or data)	19324	L3
L2	L1 and @ad<20010101	237	L2
L1	seed near5 random adj number adj generator	262	L1

END OF SEARCH HISTORY

Patent Details:
Patent No Kind Lan Pg   Main IPC   Filing Notes
US 5412730   A   12 H04L-009/00   CIP of application US 89418178
Abstract (Basic): US 5412730 A

The method provides a **seed** value to both the **transmitter** and **receiver** , which is followed by generating a first sequence of pseudo-**random** key values based on the **seed** value at the **transmitter** . Each **new** **key** value in the sequence is produced at a time dependent upon a set characteristic of the data being **transmitted** over the link.

The method also entails **encryption** the data sent over the link at the **transmitter** in accordance with the first sequence. A second sequence of pseudo- **random** key values is then generated which is based on the **seed** value at the **receiver** . Each **new** **key** value in the sequence is produced at a time dependent upon the set characteristic of the data **transmitted** over the link.

USE/ADVANTAGE - In **transmitting** data with cleat text data and **cipher** text used unique key value. Improved flexibility and security.

Dwg.1/4

Title Terms: **ENCRYPTION** ; DATA; TRANSMISSION; SYSTEM; CONTAIN; FACILITY; **RANDOM** ; ALTER; **ENCRYPTION** ; KEY; KEY; MEMORY; PERMIT; UNIQUE; SERIAL; NUMBER; IDENTIFY; REMOTE; UNIT; STORAGE; CURRENT; **ENCRYPTION** ; KEY; VALUE
Derwent Class: W01
International Patent Class (Main): **H04L-009/00**
File Segment: EPI

12/5/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009942464 **Image available**
WPI Acc No: 1994-210177/199426
Related WPI Acc No: 1993-281861; 1993-344999; 1994-110856; 1994-134066
XRPX Acc No: N94-165528

Authentication method for terminal in mobile communications system - enciphers copy of terminal key used to authenticate initial service request and stores it in terminal to authenticate subsequent requests

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Inventor: NOHARA T; SUZUKI S
Number of Countries: 005 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 604911	A2	19940706	EP 93120813	A	19931223	199426	B
JP 6204945	A	19940722	JP 92348296	A	19921228	199434	
US 5390252	A	19950214	US 93171663	A	19931222	199512	
EP 604911	A3	19950510				199546	
JP 3054282	B2	20000619	JP 92348296	A	19921228	200033	
JP 3246969	B2	20020115	JP 92348297	A	19921228	200206	
EP 604911	B1	20020828	EP 93120813	A	19931223	200264	
DE 69332238	E	20021002	DE 632238	A	19931223	200273	
			EP 93120813	A	19931223		

Priority Applications (No Type Date): JP 92348297 A 19921228; JP 92348296 A 19921228
Cited Patents: No-SR.Pub; 2.Jnl.Ref; EP 246823; EP 402083; EP 484686; JP 4264864; JP 4268848; WO 9016124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 604911	A2	E	37	H04L-009/32	
Designated States (Regional): DE FR GB					
JP 6204945	A		9	H04B-007/26	
US 5390252	A		31		
JP 3054282	B2		10	H04Q-007/38	Previous Publ. patent JP 6204945
JP 3246969	B2		13	H04L-009/32	Previous Publ. patent JP 6202864
EP 604911	B1	E		H04L-009/32	
Designated States (Regional): DE FR GB					
DE 69332238	E			H04L-009/32	Based on patent EP 604911

Abstract (Basic): EP 604911 A

The authentication method uses a communication processor (20) which retrieves a **cipher** key (Ka) from memory (30) for a terminal (10) making an initial service request. It **enciphers** the key with its own key (Kb) and **transmits** the result and a **random** number (Y1) to the terminal for respective storage and **enciphering** .

The **enciphered random** number is **transmitted** to the processing unit, which authenticates it with the retrieved key (Ka). For subsequent service requests, the terminal **transmits** a corresp. mode signal and the stored **enciphered** key. The processing unit **transmits** a second **random** number (Y2) to the terminal for **enciphering** and deciphers the **enciphered** key to authenticate the response.

USE/ADVANTAGE - Esp. for mobile telecommunications system. Authentication processing time of service requests subsequent to initial service request minimised.

Dwg.3/18

Title Terms: AUTHENTICITY; METHOD; TERMINAL; MOBILE; COMMUNICATE; SYSTEM; **ENCIPHER** ; COPY; TERMINAL; KEY; AUTHENTICITY; INITIAL; SERVICE; REQUEST; STORAGE; TERMINAL; AUTHENTICITY; SUBSEQUENT; REQUEST

Derwent Class: P85; W01

International Patent Class (Main): H04B-007/26; **H04L-009/32** ; H04Q-007/38

International Patent Class (Additional): **G06F-013/00** ; G09C-001/00; **H04L-001/02** ; **H04L-009/00** ; H04M-001/26

File Segment: EPI; EngPI

12/5/14 (Item 14 from file: 350)

DIALOG(R)File 350:Derwent WPIX

009489200 **Image available**

WPI Acc No: 1993-182735/199322

XRPX Acc No: N93-140453

Writing secure information to smart cards in remote locations - enciphering confidential information and establishing session code, then establishing second session code by user

Patent Assignee: SECURITY DOMAIN PTY LTD (SECU-N)

Inventor: BOWCOCK M P; LAING S G

Number of Countries: 039 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9310509	A1	19930527	WO 92AU608	A	19921110	199322	B
AU 9229183	A	19930615	AU 9229183	A	19921110	199340	
FI 9402177	A	19940511	WO 92AU608	A	19921110	199428	
			FI 942177	A	19940511		
NO 9401774	A	19940511	WO 92AU608	A	19921110	199429	
			NO 941774	A	19940511		
AU 656245	B	19950127	AU 9229183	A	19921110	199512	
US 5534857	A	19960709	WO 92AU608	A	19921110	199633	
			US 94232088	A	19940428		
EP 722596	A1	19960724	EP 92923477	A	19921110	199634	
			WO 92AU608	A	19921110		
EP 722596	A4	19970305	EP 92923477	A	19920000	199729	

Priority Applications (No Type Date): AU 919443 A 19911112

Cited Patents: EP 374012; EP 385400; US 4453074; EP 138386; EP 440800; WO 8801818

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9310509	A1	E	19	G06K-019/073	

Designated States (National): AT AU BB BG BR CA CH CS DE DK ES FI GB HU JP KP KR LK LU MG MN MW NL NO PL RO RU SD SE UA US

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL OA SE

AU 9229183	A	G06K-019/073	Based on patent WO 9310509
AU 656245	B	G06K-019/073	Previous Publ. patent AU 9229183 Based on patent WO 9310509

US 5534857 A 11 G07F-007/08 Based on patent WO 9310509
EP 722596 A1 E 19 G06K-019/073 Based on patent WO 9310509
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL SE
FI 9402177 A G06K-000/00
NO 9401774 A G06K-019/073
EP 722596 A4 G06K-019/073

Abstract (Basic): WO 9310509 A
Data from the issuer of a smart card at a remote location establishes a communication link between the terminal and the issuer's secure computer and a smart card reader/writer. The issuer and retailer identify each other and a session key is established to **encipher** the data between the issuer and retailer and writing from the issuer's computer to the customer smart card.
Personalisation establishes a **second** session **key** to **encipher** data traffic between the data terminal and the issuer's computer. The issuer (2) is the organisation which provides goods or services and is responsible for the system as a whole such as a bank or telecommunications operator. The retailer (3) represents the issuer and the customer (4) is the end user.
ADVANTAGE - Secure communication of personal, financial and other information using PIN unblocking keys.
Dwg.1/1
Title Terms: WRITING; SECURE; INFORMATION; SMART; CARD; REMOTE; LOCATE; **ENCIPHER** ; CONFIDE; INFORMATION; ESTABLISH; SESSION; CODE; ESTABLISH; SECOND; SESSION; CODE; USER
Derwent Class: P85; T01; T04; W01
International Patent Class (Main): G06K-000/00; G06K-019/073; G07F-007/08
International Patent Class (Additional): G09C-001/00; **H04L-009/32**
File Segment: EPI; EngPI

12/5/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008765013 **Image available**
WPI Acc No: 1991-269026/199137
XRPX Acc No: N91-205433
Continuous cipher **sync. for digital cellular communication - generating pseudo** random **key stream from multi-bit counter for combination with data and providing continuous updates to** transmitter **counter**
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF); ERICSSON OY AB L M (TELF)
Inventor: WILKINSON D P; DENT P W; DENT P W M; WILKINSON DENT P
Number of Countries: 027 Number of Patents: 027
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 446194	A	19910911	EP 91850057	A	19910306	199137	B
WO 9114315	A	19910919				199140	
SE 9000801	A	19910908				199144	
US 5060266	A	19911022	US 90556102	A	19900720	199145	
SE 465797	B	19911028				199146	
AU 9174947	A	19911010				199201	
FI 9105238	A	19911106				199207	
NO 9104313	A	19911219				199212	
BR 9104862	A	19920414	BR 914862	A	19910306	199222	
			WO 91SE173	A	19910306		
CN 1054693	A	19910918	CN 91101464	A	19910307	199225	
JP 4505694	W	19921001	JP 91505895	A	19910306	199246	
			WO 91SE173	A	19910306		
CA 2053865	A	19920907	CA 2053865	A	19910306	199248	N
PT 96968	A	19930129	PT 96968	A	19910307	199308	
AU 9331843	A	19930325	AU 9331843	A	19930115	199319	
			AU 9174947	A			
NZ 237080	A	19930526	NZ 237080	A	19910211	199324	
AU 643771	B	19931125	AU 9174947	A	19910306	199403	

AU 649908	B	19940602	AU 9174947	A	19910306	199427		
			AU 9331843	A	19930115			
EP 446194	B1	19950517	EP 91850057	A	19910306	199524		
DE 69109712	E	19950622	DE 609712	A	19910306	199530		
			EP 91850057	A	19910306			
CN 1025704	C	19940817	CN 91101464	A	19910307	199536		
ES 2073156	T3	19950801	EP 91850057	A	19910306	199537		
IE 68879	B	19960724	IE 91674	A	19910228	199644		
PH 27338	A	19930608	PH 42020	A	19910218	199721		
NO 302727	B1	19980414	WO 91SE173	A	19910306	199822		
			NO 914313	A	19911104			
KR 9611190	B1	19960821	WO 91SE173	A	19910306	199924		
			KR 91701544	A	19911107			
FI 104028	B1	19991029	WO 91SE173	A	19910306	199951		
			FI 915238	A	19911106			
CA 2053865	C	20000516	CA 2053865	A	19910306	200038	N	
			WO 91SE173	A	19910306			

Priority Applications (No Type Date): US 90556102 A 19900720; SE 90801 A 19900307; CA 2053865 A 19910306

Cited Patents: EP 273289; EP 73323; US 4549308; US 4555805; US 4633854; US 4757536; WO 8400456; US 4636854

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 446194	A				
Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL SE					
WO 9114315	A				
Designated States (National): AU BR CA FI JP KR NO					
BR 9104862	A			H04B-007/26	Based on patent WO 9104315
CN 1054693	A			H04L-009/14	
JP 4505694	W		18	H04L-009/28	Based on patent WO 9114315
CA 2053865	A			H04J-003/00	
PT 96968	A			H04B-007/26	
AU 9331843	A			H04B-007/26	Div ex application AU 9174947
NZ 237080	A			H04B-007/26	
AU 643771	B			H04B-007/26	Previous Publ. patent AU 9174947 Based on patent WO 9114315
AU 649908	B			H04B-007/26	Div ex application AU 9174947 Previous Publ. patent AU 9331843
EP 446194	B1	E	35	H04B-007/26	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL SE					
DE 69109712	E			H04B-007/26	Based on patent EP 446194
CN 1025704	C			H04L-009/14	
ES 2073156	T3			H04B-007/26	Based on patent EP 446194
IE 68879	B			H04B-007/26	
PH 27338	A			H04L-009/00	
NO 302727	B1			H04B-007/26	Previous Publ. patent NO 9104313
KR 9611190	B1			H04B-007/26	
FI 104028	B1			H04B-007/26	Previous Publ. patent FI 9105238
CA 2053865	C	E		H04J-003/00	Based on patent WO 9114315

Abstract (Basic): EP 446194 A

A first pseudo- **random** key stream of bits is generated in accordance with an algorithm that is a function of a multi-bit digital value contained in a first register. The value in the register is incremented at regular periodic intervals to vary the pattern of bits in the key stream. The bits of the key stream are combined with a stream of data bits carrying communications information to cryptographically encode the data and the encoded data is **transmitted** to a **receiver** . Also **transmitted** to the **receiver** at regular periodic intervals and interspersed with the transmission of encoded data is the value contained in the register, a **second** pseudo- **random** **key** stream of bits is generated in accordance with the algorithm which is the function of a multi-bit digital value contained in a second register.

The value in the second register is incremented at the same intervals as the first register to vary the pattern of bits in the second stream in an identical fashion to the pattern in the first

stream. The bits of the second stream are combined with the **received** stream of encoded data to decode the data into the communications information. The value contained in the second register is periodically compared with the **received** value of the first register to determine whether the two values match for corresponding moments of time and whether the first and **second** **key** streams are in synchronism with one another.

ADVANTAGE - Prevents accumulation of errors by providing continuous or very frequent updates to reset **receiver** counter and to resynchronise system without necessity of reinitialisation and repetition of intervening clock pulses.

Dwg.6/9

Title Terms: CONTINUOUS; **CIPHER** ; SYNCHRONOUS; DIGITAL; CELLULAR; COMMUNICATE; GENERATE; PSEUDO; **RANDOM** ; KEY; STREAM; MULTI; BIT; COUNTER ; COMBINATION; DATA; CONTINUOUS; UPDATE; **TRANSMIT** ; COUNTER

Derwent Class: W01; W02

International Patent Class (Main): H04B-007/26; H04J-003/00; **H04L-009/00** ; **H04L-009/14** ; **H04L-009/28**

International Patent Class (Additional): **H04K-001/00** ; **H04L-007/04** ; **H04L-009/18** ; H04Q-007/02

File Segment: EPI

12/5/16 (Item 16 from file: 350)

DIALOG(R)File 350:Derwent WPIX

008382533 **Image available**

WPI Acc No: 1990-269534/199036

XRPX Acc No: N90-208616

Cipher **key distribution system - stores public information on common file and has two sub-systems with** transmitters **and** receivers

Patent Assignee: NEC CORP (NIDE)

Inventor: TANAKA K

Number of Countries: 008 Number of Patents: 009

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 385511	A	19900905	EP 90104200	A	19900305	199036	B
AU 9050706	A	19900906				199043	
CA 2011396	A	19900903				199047	
JP 3016339	A	19910124	JP 9050939	A	19900302	199110	
US 5029208	A	19910702	US 90488952	A	19900305	199129	
EP 385511	A3	19920603	EP 90104200	A	19900305	199332	
CA 2011396	C	19950103	CA 2011396	A	19900302	199510	
EP 385511	B1	19970806	EP 90104200	A	19900305	199736	
DE 69031185	E	19970911	DE 631185	A	19900305	199742	
			EP 90104200	A	19900305		

Priority Applications (No Type Date): JP 8980501 A 19890330; JP 8952352 A 19890303; JP 8952353 A 19890303; JP 8952354 A 19890303; JP 9050939 A 19900302

Cited Patents: NoSR.Pub; 1.Jnl.Ref; EP 257585

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 385511	A				
Designated States (Regional): DE FR GB NL					
EP 385511	B1	E	23	H04L-009/08	
Designated States (Regional): DE FR GB NL					
DE 69031185	E			H04L-009/08	Based on patent EP 385511
CA 2011396	C			H04L-009/08	

Abstract (Basic): EP 385511 A

A system includes a common file for storing public information in a position indicated by the **receiving** party identifying information. A **transmitting** subsystem is capable of reading the common file, generating **random** numbers and a **cipher** key, and storing secret information. The subsystem also generates a key distribution code and **transmits** this code together with information identifying the communicating party.

A **receiving** subsystem **receives** the key distributing code and identifies information, stores a constant and secret information and generates the same **cipher** key as the **transmitting** subsystem.

USE/ADVANTAGE - For one way communication system. Avoids excessive overheads and improves security.

Dwg.2/11

Title Terms: **CIPHER** ; KEY; DISTRIBUTE; SYSTEM; STORAGE; PUBLIC; INFORMATION; COMMON; FILE; TWO; SUB; SYSTEM; **TRANSMIT** ; **RECEIVE**
Derwent Class: P85; W01
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): G09C-001/00; **H04K-001/00**
File Segment: EPI; EngPI

12/5/17 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008374069 **Image available**
WPI Acc No: 1990-261070/199034
XRPX Acc No: N90-202257

Data communication apparatus using data carrier - uses session key generated from random **number forming appts.** ciphered **using master key, in external unit**

Patent Assignee: MATSUSHITA ELEC IND CO LTD (MATU)
Inventor: ITO M; TAKAGI N; TSUJI T
Number of Countries: 002 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9009009	A	19900809				199034	B
EP 422230	A	19910417	EP 90902392	A	19900124	199116	
US 5227613	A	19930713	WO 90JP78	A	19900124	199329	
			US 90582172	A	19901120		
KR 9305572	B1	19930623	WO 90JP78	A	19900124	199425	
			KR 90702115	A	19900924		
EP 422230	A4	19960703	EP 90902392	A	19900000	199644	

Priority Applications (No Type Date): JP 8915336 A 19890124; JP 8915329 A 19890124
Cited Patents: JP 60062252; JP 62189593; JP 62191991; JP 63050222; JP 63131169; JP 63219244; EP 114368; EP 128672; EP 138219; EP 147337; EP 166541; EP 281059; EP 284133; EP 292249; EP 305004; EP 55986; FR 2536928
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5227613	A		18	H04L-009/12	Based on patent WO 9009009
KR 9305572	B1			G06K-019/073	

Abstract (Basic): WO 9009009 A

To prevent eavesdropping of data from the communication wire, a session key (rl) generated from a **random** number forming device (15) is **ciphered** (16) using a master key (km) and is sent to an external unit. Further, a cryptogram input from an external unit is decoded (17) using a session key (rl) generated from the **random** number forming device (15). (50pp Dwg.No.2/11)

Title Terms: DATA; COMMUNICATE; APPARATUS; DATA; CARRY; SESSION; KEY; GENERATE; **RANDOM** ; NUMBER; FORMING; APPARATUS; MASTER; KEY; EXTERNAL; UNIT
Derwent Class: P85; T04; W01; W02
International Patent Class (Main): G06K-019/073; **H04L-009/12**
International Patent Class (Additional): G06K-017/00; G06K-019/07; G09C-001/00
File Segment: EPI; EngPI

12/5/18 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008332139 **Image available**
WPI Acc No: 1990-219140/199029
XRPX Acc No: N90-170043
Certification system for IC card memory - sends random **number**, encryption **algorithm selector and key data between terminal and card to certify terminal**
Patent Assignee: TOSHIBA KK (TOKE)
Inventor: IIJIMA Y
Number of Countries: 004 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2227111	A	19900718	GB 8929239	A	19891228	199029	B
JP 2187785	A	19900723	JP 898011	A	19890117	199035	
FR 2641885	A	19900720				199036	
GB 2227111	B	19930519	GB 8929239	A	19891228	199320	
US 5293029	A	19940308	US 90463601	A	19900111	199410	
			US 91747420	A	19910819		
			US 92942337	A	19920909		

Priority Applications (No Type Date): JP 898011 A 19890117; JP 898010 A 19890117
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5293029	A		22	G06K-005/00	Cont of application US 90463601
					Cont of application US 91747420
GB 2227111	B			G07F-007/08	

Abstract (Basic): GB 2227111 A
The certification system includes an electronic device with at least one **key** data. A **second** electronic device is capable of performing communication with the first electronic device. The first data and designation data fro designating key data for **encrypting** the first data is **transmitted** from the second electronic device to the first electronic device.
When the first data and the designation data are **received** by the first electronic device, one key data from the at least one key data in accordance with the **received** designation data is selected and the **received** first data is **encrypted** by using the selected key data. Part of the **encrypted** data is **transmitted** to the second electronic device after the first data is entirely **received** by the first electronic device.
USE - For IC cards using erasable non-volatile and control element.
Dwg.1/8
Title Terms: CERTIFY; SYSTEM; IC; CARD; MEMORY; **SEND** ; **RANDOM** ; NUMBER; **ENCRYPTION** ; ALGORITHM; SELECT; KEY; DATA; TERMINAL; CARD; CERTIFY; TERMINAL
Derwent Class: P85; T01; T04; T05
International Patent Class (Main): G06K-005/00; G07F-007/08
International Patent Class (Additional): G06K-019/07; G09C-001/00; **H04L-009/14** ; **H04L-009/32**
File Segment: EPI; EngPI

12/5/19 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007487208
WPI Acc No: 1988-121141/198818
XRPX Acc No: N88-091961
Telecommunication security system and key memory module - matches codes from security units associated with service and user to open transmission gate
Patent Assignee: MANITOBA TELEPHONE SYSTEM (MANI-N); COMPUTREX CENT LTD (COMP-N)
Inventor: LEMIRE J R; POLLARD J A
Number of Countries: 016 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 266044	A	19880504	EP 87307833	A	19870904	198818	B
JP 63139440	A	19880611	JP 87221800	A	19870904	198829	
US 4897875	A	19900130	US 8792625	A	19870903	199012	
CA 1283187	C	19910416				199120	
EP 266044	B1	19931229	EP 87307833	A	19870904	199401	
DE 3788621	G	19940210	DE 3788621	A	19870904	199407	
			EP 87307833	A	19870904		

Priority Applications (No Type Date): GB 8621333 A 19860904
Cited Patents: 1.Jnl.Ref; A3...9029; EP 194782; GB 2099195; No-SR.Pub; US 4310720; US 4484306; WO 8302343
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 266044	A	E	23		
Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL SE					
US 4897875	A		19		
EP 266044	B1	E	22	H04M-001/66	
Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL SE					
DE 3788621	G			H04M-001/66	Based on patent EP 266044

Abstract (Basic): EP 266044 A

A security system for authenticating a potential user of a service has a first unit associated with the service and a second unit associated with the user. Each unit communicates with the other through a communication medium. Each unit includes a memory, at least one of the units including a memory module and having stored groups of **random** numbers. The numbers of each group are logically associated as a group at a logical address. The **random** numbers and associated addresses in the memory of the first unit are identical to those of the memory of the second unit.

The first unit has a control circuit to extract from the memory one of the **random** numbers to communicate the number to the second unit, compare a **received** signal from the second unit with another of the **random** numbers, and to provide authentication of the user only upon the match of the **received** signal with the other **random** numbers. In each subsequent cycle of operation it extracts one of the **random** numbers from a different group. The second unit includes a control circuit arranged on receipt from the first unit of the **random** numbers to extract from its memory another **random** number of the group.

USE/ADVANTAGE - For **encryption** , authentication, identification and/or digital signature. Allows **encryption** keys to be exchanged or transferred in any open communications environment (e.g. telephone, radio, etc.) without providing any information that attacker could use to discover keys, accommodates very rapid (less than one **second**) **key** changes at any time during established session.

2/8

Title Terms: TELECOMMUNICATION; SECURE; SYSTEM; KEY; MEMORY; MODULE; MATCH; CODE; SECURE; UNIT; ASSOCIATE; SERVICE; USER; OPEN; TRANSMISSION; GATE
Derwent Class: W01
International Patent Class (Main): H04M-001/66
International Patent Class (Additional): **G06F-001/00** ; **H04L-009/02**
File Segment: EPI

12/5/20 (Item 20 from file: 350)

007423896 **Image available**
WPI Acc No: 1988-057831/198809
XRPX Acc No: N88-043955

Key distribution method for enciphering **plain text message - generating key distribution information by applying predetermined transformation to** random **number on basis of secret information**

Patent Assignee: NEC CORP (NIDE)
Inventor: OKAMOTO E

Number of Countries: 007 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 257585	A	19880302	EP 87112158	A	19870821	198809	B
JP 63054037	A	19880308	JP 86197610	A	19860822	198815	
JP 63054038	A	19880308	JP 86197611	A	19860822	198815	
US 4876716	A	19891024	US 8788319	A	19870824	199001	
CA 1279709	C	19910129				199110	
EP 257585	B1	19921125	EP 87112158	A	19870821	199248	
DE 3782780	G	19930107	DE 3782780	A	19870821	199302	
			EP 87112158	A	19870821		

Priority Applications (No Type Date): JP 86197611 A 19860822; JP 86197610 A 19860822
Cited Patents: 3.Jnl.Ref; A3...8850; EP 197392; JP 61030829; No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 257585	A	E	8		
Designated States (Regional): BE DE FR GB					
US 4876716	A		9		
EP 257585	B1	E	11	H04L-009/08	
Designated States (Regional): BE DE FR GB					
DE 3782780	G			H04L-009/08	Based on patent EP 257585

Abstract (Basic): EP 257585 A

The key distribution method comprises generating a **random** number in one system and generating key distribution information in the system by applying a predetermined transformation the **random** number on the basis of secret information known only by the system. The information is **transmitted** to a further system via a communication channel and is **received** in the second system, where another **random** number is generated.

Further key distribution information is generated by applying the first transformation to the second **random** number on the basis of secret information known only by the second system. The information is **transmitted** to the first system. An **enciphering** key is generated by applying a predetermined transformation to the information on the basis of the first **random** number and ID information of the non-secret further information.

1/3

Title Terms: KEY; DISTRIBUTE; METHOD; **ENCIPHER** ; PLAIN; TEXT; MESSAGE; GENERATE; KEY; DISTRIBUTE; INFORMATION; APPLY; PREDETERMINED; TRANSFORM; **RANDOM** ; NUMBER; BASIS; SECRET; INFORMATION
Index Terms/Additional Words: **ENCRYPTI ON_DEC RYPTER8809** ; DECRYPTER
Derwent Class: W01
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): **H04K-001/00**
File Segment: EPI

12/5/21 (Item 21 from file: 350)
DIALOG(R)File 350:Derwent WPIX

004770002
WPI Acc No: 1986-273343/198642
XRPX Acc No: N86-204056
Cryptographic communication appts. for duplex transmission - establishes single use session keys for authenticating users or terminals at remote locations
Patent Assignee: IBM CORP (IBMC)
Inventor: BASS W E; MATYAS S M; OSEAS J
Number of Countries: 007 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 197392	A	19861015	EP 86103847	A	19860321	198642	B
JP 61237546	A	19861022	JP 8658460	A	19860318	198649	
US 4649233	A	19870310	US 85722091	A	19850411	198712	

CA 1249865	A	19890207	198908
EP 197392	B	19911116	199145
DE 3682309	G	19911212	199151

Priority Applications (No Type Date): US 85722091 A 19850411
Cited Patents: 1.Jnl.Ref; A3...8850; EP 100260; EP 35448; EP 64779; EP 90771; GB 2099195; No-SR.Pub; 1.Jnl.REf; EP 64779; EP 90771
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 197392	A	E	20		
Designated States (Regional): DE FR GB IT					
EP 197392	B				
Designated States (Regional): DE FR GB IT					

Abstract (Basic): EP 197392 B

A session key is valid only for the duration of a single cryptographic session. Each node has a local cryptographic facility including a predetermined cross-domain key and an attribute associated with the other node/user identity.

A **random** number is generated and **encrypted** under the cross-domain key. The **encrypted** number is copied to the other node. Any **received encrypted random** number from the other node is decrypted under the cross-domain key. A parameter is formed by combining the attributes derived or associated with the identities of both nodes/users. An interim key is formed from the composite of the local and **received random** numbers. The parameter is combined with the interim key to produce the session key.

ADVANTAGE - reduces vulnerability to both playback and password attack. (20pp Dwg.No.2/4

Title Terms: CRYPTOGRAPHIC; COMMUNICATE; APPARATUS; DUPLEX; TRANSMISSION; ESTABLISH; SINGLE; SESSION; KEY; AUTHENTICITY; USER; TERMINAL; REMOTE; LOCATE
Derwent Class: W01
International Patent Class (Additional): **H04L-009/00**
File Segment: EPI

12/5/22 (Item 22 from file: 350)

004411386
WPI Acc No: 1985-238264/198539
XRPX Acc No: N85-178239
De-scrambler subscriber key production system - uses key seeds **stored in secure memory in de-scrambler and subscriber key generator**
Patent Assignee: CABLE HOME COMMUNICATION CORP (CABL-N); TITAN CORP (TITA-N); CABLE HOME COMMUNICATION (CABL-N); M/A-COM LINKABIT IN (MACO-N)
Inventor: MOERDER K E; MOEDER K E
Number of Countries: 017 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 155762	A	19850925	EP 85300983	A	19850214	198539	B
AU 8539540	A	19850919				198545	
NO 8500986	A	19851007				198547	
DK 8500850	A	19850916				198550	
JP 61016643	A	19860124	JP 8548433	A	19850313	198610	
US 4634808	A	19870106	US 84589741	A	19840315	198704	
CA 1225458	A	19870811				198736	
EP 155762	B	19900725				199030	
DE 3578792	G	19900830				199036	
DK 166247	B	19930322	DK 85850	A	19850225	199317	

Priority Applications (No Type Date): US 84589741 A 19840315
Cited Patents: 2.Jnl.Ref; A3...8722; EP 127381; No-SR.Pub; US 4388643
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 155762	A	E	24		

Designated States (Regional): AT BE CH DE FR GB IT LI LU NL SE
EP 155762 B
Designated States (Regional): AT BE CH DE FR GB IT LI LU NL SE
DK 166247 B H04N-007/167 patent DK 8500850

Abstract (Basic): EP 155762 A

A scrambled signal is **received** together with an **encrypted** key signal, a key generation number and an address for accessing a predetermined area in a memory. A circuit provides a subscriber key generation signal that is unique to the descrambler. A generator reproduces the unique subscriber key signal by processing the subscriber key generation signal in accordance with a predetermined **encryption** algorithm, on the algorithm being keyed by a prescribed subscriber a key **seed** signal unique to the descrambler.

A memory stores the prescribed subscriber key **seed** signal and provides it to key the algorithm when the memory is accessed by the address **received** with the key generation number. A circuit accesses the memory with the address reserved with the key generation number.

USE/ADVANTAGE - For e.g. controlling distribution of scrambled signals in television subscription system. Has reduced probability ofunauthorised ascertainment and use of key signal.

2/4

Title Terms: DE; SCRAMBLE; SUBSCRIBER; KEY; PRODUCE; SYSTEM; KEY; **SEED** ; STORAGE; SECURE; MEMORY; DE; SCRAMBLE; SUBSCRIBER; KEY; GENERATOR
Derwent Class: W02; W03
International Patent Class (Main): **H04N-007/167**
International Patent Class (Additional): **H04K-001/00** ; **H04L-009/04** ; **H04N-007/16**
File Segment: EPI

12/5/23 **(Item 23 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

003923485
WPI Acc No: 1984-069029/198411
XRPX Acc No: N84-052006

Coded data transmission system - randomises **information-containing data signal for transmission and for reproducing it at** receiver **using scrambler-on** encryption **system**

Patent Assignee: RACAL DATA COMMUNICATIONS INC (RACA)
Inventor: FERRELL P J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 4434322	A	19840228	US 81286356	A	19810723	198411	B

Priority Applications (No Type Date): US 81286356 A 19810723; US 65481021 A 19650819; US 83557915 A 19831205
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 4434322	A		13		

Abstract (Basic): US 4434322 A

The information-containing data to be **transmitted** is applied to a modulo-two adder, the output of which is the encoded data for transmission and which is also an input of an n stage shift register. An arbitrary logic network, having several inputs each connected to several selected shift register stages, produces a particular key signal responsive to the condition of the contents of the selected shift register stages. At the **receiver** , the **received randomized** data is fed simultaneously to the input of an n stage shift register and to an input of a modulo-two adder.

An identical arbitrary logic network is connected to the **receiver** shift register and produces the same particular key signal responsive to the same conditions in the shift register. The modulo-two adder in the **receiver** has as its **second** input the **key** signal. The use of

the scrambler/ **encryption** circuitry may be for other applications, i.e. rendering tamperproof recorded information, e.g. audio recording, and checking the operation of high speed shift registers.
0/4
Title Terms: CODE; DATA; TRANSMISSION; SYSTEM; **RANDOM** ; INFORMATION; CONTAIN; DATA; SIGNAL; TRANSMISSION; REPRODUCE; **RECEIVE** ; SCRAMBLE; **ENCRYPTION** ; SYSTEM
Index Terms/Additional Words: **SECRET** ; **PRIVATE** ; **RADIO**
Derwent Class: W01; W02
International Patent Class (Additional): **H04L-009/00**
File Segment: EPI

12/5/24 (Item 24 from file: 347)
DIALOG(R)File 347:JAPIO

07575717 **Image available**
INFORMATION PROVIDING DEVICE, INFORMATION DISTRIBUTING TERMINAL, INFORMATION PROVIDING METHOD, COMPUTER PROGRAM, AND STORAGE MEDIUM

PUB. NO.: 2003-069558 [JP 2003069558 A]
PUBLISHED: March 07, 2003 (20030307)
INVENTOR(s): YAMANAKA YASUHIRO
YOSHITOMI KAZUNORI
HISAMATSU FUMIAKI
APPLICANT(s): SONY CORP
APPL. NO.: 2001-251588 [JP 2001251588]
FILED: August 22, 2001 (20010822)
INTL CLASS: **H04L-009/32** ; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/30** ; **G06F-017/60** ; G09C-001/00; **H04L-009/08** ; **H04N-005/76** ; **H04N-007/173**

ABSTRACT
PROBLEM TO BE SOLVED: To provide an information distribution system capable of preventing unauthorized copying.

SOLUTION: An information providing device 182 provides content data recorded in an information distributing terminal 400 to a predetermined storage medium. External authentication for the information providing device 182 can be conducted securely by providing a key holding means 4222 for securely holding a first external authentication key, a **random** number generating means 4223 for generating a **random** number, an **encrypting** means 4224 for **encrypting** a **random** number using the first external authentication key to generate a first **encrypted** data, a means for **transmitting** a **random** number to the information distributing terminal, a reception means 4227 for **receiving** a second **encrypted** data obtained in **encryption** of a **random** number by the information distributing terminal using a **second** external authentication **key** same as the first external authentication key, and a comparing means 4226 for comparing the first **encrypted** data and the second **encrypted** data.

12/5/25 (Item 25 from file: 347)
DIALOG(R)File 347:JAPIO

07475920 **Image available**
KEY SHARING SYSTEM, KEY SHARING DEVICE AND PROGRAM THEREOF

PUB. NO.: 2002-344438 [JP 2002344438 A]
PUBLISHED: November 29, 2002 (20021129)
INVENTOR(s): HIRATA SHINICHI
AKASHIKA HIDEKI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)
APPL. NO.: 2001-143830 [JP 2001143830]

FILED: May 14, 2001 (20010514)
INTL CLASS: **H04L-009/08**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a key sharing technology for connecting safe **enciphered** communication path by using a public key cryptograph between arbitrary devices.

SOLUTION: In a key sharing system having a first device and a **second** device, public **key** certificates are exchanged, and a first device generates a first **random** number, and generates first data by **enciphering** the first **random** number with the public **key** of a **second** device, and **transmits** the first data to a second device. The second device acquires the first **random** number, by decoding the first data with the secret **key** of the **second** device, and generates a second **random** number, generates a session key from the first **random** number and the second **random** number, generates second data by **enciphering** the generated second **random** number with the public key of the first device, and **transmits** the second data to the first device. The first device acquires the second **random** number, by decoding the **received** second data with the secret key of the first device, and generates a session **key** from the **second random** number and the first **random** number.

12/5/26 (Item 26 from file: 347)

07349399 **Image available**
METHOD OF FINDING REPLICATED TERMINAL

PUB. NO.: 2002-217890 [JP 2002217890 A]
PUBLISHED: August 02, 2002 (20020802)
INVENTOR(s): MATSUZAKI NATSUME
ANZAI JUN
MATSUMOTO TSUTOMU
APPLICANT(s): ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
APPL. NO.: 2001-013250 [JP 200113250]
FILED: January 22, 2001 (20010122)
INTL CLASS: **H04L-009/08** ; G09C-001/00; **H04L-009/32**

ABSTRACT

PROBLEM TO BE SOLVED: To automatically find and exclude a replicated terminal in a communication system consisting of a center and a plurality of terminals.

SOLUTION: The center and a plurality of the terminal are connected through a communication network for **ciphering** communication with individual group keys. The center **sends** challenge information, in the case of **delivering** a **new** group **key** to the terminals. Each of the terminals **sends** response information obtained by **ciphering** terminal ID and a terminal **random** number to a center public key to the center, which retrieves a communication log to inspect the presence/absence of terminals, having the same terminal ID and different terminal **random** numbers. If there are corresponding terminals, it is determined that the replicated terminal exists, and the session key is not **delivered** . Since **random** number generated by an original terminal is difficult to replicate, the replicated terminal cannot generate the same **random** number, so that the existence of the replicated terminal can be detected. When the replicated terminal is found, the multi-address communication of exclusion information that this has been excluded is performed, to **deliver** the same group keys to unchecked terminals.

12/5/27 **(Item 27 from file: 347)**
DIALOG(R)File 347:JAPIO

07349397 **Image available**
METHOD FOR FINDING REPLICATED TERMINAL

PUB. NO.: 2002-217888 [JP 2002217888 A]
PUBLISHED: August 02, 2002 (20020802)
INVENTOR(s): ANZAI JUN
MATSUZAKI NATSUME
MATSUMOTO TSUTOMU
APPLICANT(s): ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
APPL. NO.: 2001-011089 [JP 200111089]
FILED: January 19, 2001 (20010119)
INTL CLASS: **H04L-009/08** ; **G06F-012/14** ; **G06F-015/00** ; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To automatically find and exclude a replicated terminal in a communication system, consisting of a center and a plurality of terminals.

SOLUTION: The center and a plurality of the terminal are connected through a communication network for **ciphering** communication with individual session keys. The center **sends** challenge information in the case of **delivering** a **new** session **key** to the terminals. Each of the terminals **sends** response information obtained by **ciphering** terminal ID and a terminal **random** number to a center public key to the center, which retrieves a communication log and inspects the presence/absence of terminals, having the same terminal ID and different terminal **random** numbers. If corresponding terminals exist, it decides that the replicated terminal exists, and the session key will not be **delivered** . Since **random** number generated by an original terminal is difficult to replicate, the replicated terminals cannot generate the same **random** number. Thus, the existence of the replicated terminal can be detected.

12/5/28 **(Item 28 from file: 347)**
DIALOG(R)File 347:JAPIO

06527864 **Image available**
RECORDING DEVICE AND ITS METHOD, DECRYPTION DEVICE AND ITS METHOD, PROVISION MEDIUM AS WELL AS INFORMATION RECORDING MEDIUM

PUB. NO.: 2000-113587 [JP 2000113587 A]
PUBLISHED: April 21, 2000 (20000421)
INVENTOR(s): ISHIBASHI YOSHITO
ASANO TOMOYUKI
KITAMURA IZURU
KITAHARA ATSUSHI
APPLICANT(s): SONY CORP
APPL. NO.: 10-282226 [JP 98282226]
FILED: October 05, 1998 (19981005)
INTL CLASS: G11B-020/10; G09C-001/00; **H04L-009/14** ; **H04L-009/32**

ABSTRACT

PROBLEM TO BE SOLVED: To enable the utilization of **encrypted** information in devices exclusive of a device to which the information is supplied while preventing the illicit utilization thereof by executing mutual authentication with an information memory medium, **encrypting** a first **key** with a **second** **key** and recording the **encrypted** information and the **encrypted** first key to the memory medium.

SOLUTION: An **encryption** section 15 reads a key for movement out of the memory section 21 of an IC card 4, again **encrypts** the decrypted content key with the key for movement and records the key on an optical disk 5. When the ID read out of the ID memory section 23 of the IC card 4 is decided to be not registered in an ID identification section 18 and is decided to be not mutually authenticated with the IC card 4, the ID identification section 18 or a mutual authentication section 17 executes prescribed error processing. The mutual authentication section 17 decrypts **received** **random** numbers with the previously stored common key and if the **random** numbers coincide with the **random** numbers before the **encryption** , the IC card 4 is authethenticated as the correct IC card.

12/5/29 (Item 29 from file: 347)
DIALOG(R)File 347:JAPIO

05716778 **Image available**
AUTHENTICATION METHOD AND SYSTEM

PUB. NO.: 09-331578 [JP 9331578 A]
PUBLISHED: December 22, 1997 (19971222)
INVENTOR(s): NAKADA KAZUHIKO
SUZUKI SHIGEFUSA
NAKANISHI TAKAO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-147699 [JP 96147699]
FILED: June 10, 1996 (19960610)
INTL CLASS: [6] H04Q-007/38; G09C-001/00; G09C-001/00; **H04L-009/08** ; **H04L-009/32**
JAPIO CLASS: 44.2 (COMMUNICATION -- Transmission Systems); 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To allow a specific subscriber to be authenticated for **receiving** the service of a plurality of communication enterprises (so-called roaming) by **sending** a **ciphered** signal from a 1st communication network and using a tentative authentication **key** in a **2nd** communication network so as to authenticate the subscriber based on a signal resulting from decoding the **ciphered** signal by the subscriber.

SOLUTION: A 2nd network **receiving** an identification number ID from a subscriber 300 **sends** the ID to a 1st network (S202). The 1st network generates a tentative anthetication key Kt and **sends** an authentication signal **ciphered** by issuing an authentication key K13 shared in common among subscribers 300 to the 2nd network (S203). The 2nd network generates a **random** number and **sends** the **random** number and the authentication number to the subscriber 300 (S204). The subscriber 300 uses the authentication key K13 to decode a tentative authentication key Kt and **ciphers** the **random** number to generate an authentication reply signal and returns the authentication reply signal to the 2nd network (S205). The 2nd network collates the authentication reply signal with the value resulting from **ciphering** the **random** number and authenticates the subscriber 300 to be a regular subscriber when they are coincident.

12/5/30 (Item 30 from file: 347)
DIALOG(R)File 347:JAPIO

05590619 **Image available**
METHOD FOR STORING AND MANAGING SECRET KEY

PUB. NO.: 09-205419 [JP 9205419 A]
PUBLISHED: August 05, 1997 (19970805)

INVENTOR(s): SHIYOUJI NAGAYOSHI
APPLICANT(s): NRI & NCC CO LTD [420135] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-011913 [JP 9611913]
FILED: January 26, 1996 (19960126)
INTL CLASS: [6] **H04L-009/08** ; G09C-001/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 44.9 (COMMUNICATION -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To disable a theft or illegal use of a secret key by devising a method such that the secret key cannot be decoded by the pass phrase of a user only and a remaining part of a decoding key is not in existence around the user

SOLUTION: When the user uses a secret key, the user inputs the pass phrase to its own computer and uses a public key of an opposite party to **cipher** a text and **sends** the resulting text. The opposite party **receiving** it returns a **random** number having **received** and stored at the end of a preceding communication. The user synthesizes a 1st scramble key from the both to decode the stored secret key and to acquire the secret key not **ciphered** . The user computer generates a 2nd **random** number and a **2nd** scramble **key** based on it and the pass phrase, **ciphers** again the secret key and stores the result. Furthermore, the 2nd **random** number is **ciphered** and sent for the use of the succeeding communication and it is deleted with the **2nd** scramble **key** from its own computer. Thus, every time a secret key, it is stored while being changed into another form.

12/5/31 (Item 31 from file: 347)
DIALOG(R)File 347:JAPIO

04425982 **Image available**
CERTIFYING METHOD FOR MOBILE COMMUNICATION SYSTEM

PUB. NO.: 06-069882 [JP 6069882 A]
PUBLISHED: March 11, 1994 (19940311)
INVENTOR(s): SUZUKI SHIGEFUSA
NOHARA TATSUO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-220386 [JP 92220386]
FILED: August 19, 1992 (19920819)
INTL CLASS: [5] H04B-007/26; **H04L-009/06** ; **H04L-009/14**
JAPIO CLASS: 44.2 (COMMUNICATION -- Transmission Systems); 26.2 (TRANSPORTATION -- Motor Vehicles); 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 1562, Vol. 18, No. 318, Pg. 111, June 16, 1994 (19940616)

ABSTRACT

PURPOSE: To secure the privacy of a certification key shared with a mobile subscriber by performing certification corresponding to a signal **receiving** and **ciphering** a temporary certification **key** from a **second** mobile communication network in the case of subscriber certification for roaming.

CONSTITUTION: When a mobile subscriber 30 moves from a first mobile communication network to a second mobile communication network 20, an identification number ID is **transmitted** for getting subscriber certification. The second network **sends** this ID and a set certification key K12 to the first network 10, and the first network returns a certification key K13 **ciphered** by the K12 to the second network in place of directly **sending** the certification key K12 shared with the subscriber 30. The second network 20 stores the K13, **sends** a **random** value to the subscriber 30, collates the **random** number value provided by restoring a certification response signal **ciphered** by the K13 by using the K12 and certifies the identity of the subscriber by the coincidence. Thus, since

the certification key K13 is used only for **ciphering** , the privacy can be secured.

12/5/32 **(Item 32 from file: 347)**
DIALOG(R)File 347:JAPIO

03371740 **Image available**
METHOD AND DEVICE FOR CONFIDENTIAL FACSIMILE COMMUNICATION

PUB. NO.: 03-034640 [JP 3034640 A]
PUBLISHED: February 14, 1991 (19910214)
INVENTOR(s): NAKAO KOJI
TANAKA TOSHIAKI
HACHITSUKA YOTARO
APPLICANT(s): KOKUSAI DENSHIN DENWA CO LTD <KDD> [000121] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 01-166933 [JP 89166933]
FILED: June 30, 1989 (19890630)
INTL CLASS: [5] **H04L-009/06 ; H04L-009/14 ; H04N-001/44**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.7 (COMMUNICATION -- Facsimile)
JOURNAL: Section: E, Section No. 1061, Vol. 15, No. 165, Pg. 27, April 25, 1991 (19910425)

ABSTRACT

PURPOSE: To facilitate the confidential communication by **enciphering** an identifier by a first **cipher** key from a **receiving** terminal and **transmitting** it to a **transmitting** terminal, **enciphering** **transmitting** document information by a **second** **cipher** **key** in the **transmitting** terminal and **transmitting** it to the **receiving** terminal.

CONSTITUTION: A **cipher** part 9 is provided with an **enciphering** circuit 13, a decoding circuit 14, a **cipher** key generating/managing circuit 15, and a pseudo **random** digit generating/ managing circuit 16. In this state, a **random** digit generated by a **transmitting** terminal is **transmitted** to a **receiving** terminal and based on its **random** digit, the same first **cipher** key is generated by both the **transmitting** and the **receiving** terminals, and identifier information of the **receiving** terminal is **enciphered** by a first **cipher** key and **transmitted** to the **transmitting** terminal. In the **transmitting** terminal, an identifier of the **receiving** terminal is decoded by using a first **cipher** key and a format is inspected, and thereafter, by displaying it on a display part 11, a **transmitting** terminal user certifies the **receiving** terminal to be the other proper party. Also, as for document information sent by a facsimile, based on the **random** digit and the identification number of the **receiving** side, a **second** **cipher** **key** is generated, and **encipherment** /decoding are executed by using it by the **transmitting** side/ **receiving** side, respectively. In such a way, tapping is prevented.

12/5/33 **(Item 33 from file: 347)**
DIALOG(R)File 347:JAPIO

02592444 **Image available**
KEY DISTRIBUTION SYSTEM

PUB. NO.: 63-209344 [JP 63209344 A]
PUBLISHED: August 30, 1988 (19880830)
INVENTOR(s): TAKEDA YUKIO
TAKANO TAKESHI
AKIYAMA RYOTA
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 62-043987 [JP 8743987]
FILED: February 26, 1987 (19870226)

INTL CLASS: [4] **H04L-009/02**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 698, Vol. 12, No. 498, Pg. 141, December 24, 1988 (19881224)

ABSTRACT

PURPOSE: To enhance the security against the interception by a 3rd party by generating a common key to a master station and each slave station at every slave station, allowing the master station to use the common key and **enciphering** a **random** number so as to **send** the result to each slave station.

CONSTITUTION: A **random** number generator 12 generates **random** numbers Xk, R and a power calculation circuit 13 applies power calculation in obtaining, e.g., common keys KA, KB. The master station generates a key Yc from a secret key Xk generated from a **random** number, **sends** it to each slave station and keys KA, KB are generated from keys Y(sub 1), Y(sub 2) based on the secret keys XA, XB of each slave station. The slave station uses the key Yc to generate **new keys** KA, KB and the master station uses the common keys KA, KB with each slave station to encript the **random** number R and **sends** the result to each slave station. Each slave station decodes the **random** number R to use the **random** number R as the common key of each slave station. Thus, the possibility of the **random** number R decoded by an intercepting personnel is decreased.

12/5/34 (Item 34 from file: 347)

01695450 **Image available**
CIPHERING DEVICE

PUB. NO.: 60-173950 [JP 60173950 A]
PUBLISHED: September 07, 1985 (19850907)
INVENTOR(s): OKAMOTO EIJI
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 59-029734 [JP 8429734]
FILED: February 20, 1984 (19840220)
INTL CLASS: [4] **H04L-009/02**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 374, Vol. 10, No. 11, Pg. 34, January 17, 1986 (19860117)

ABSTRACT

PURPOSE: To eliminate the need for additional registration of a **new key** by scrambling a **random** number, encoding and decoding data depending on an opposite terminal device address and the storage content of a storage means in a encoding device distributing a key for encoding.

CONSTITUTION: A multiplexer 102 gives (i, j) as the result of arrangement of an opposite side terminal address (j) and an own terminal address (i) of an address memory 103 as a bit pattern to an exclusive OR element 104 to form (i, j)+ MK=Kij to a master key MK of a memory 105. A scrambler 106 **transmits** the result scrambling the **random RN** generated by a **random** number generator 101 by using a bit pattern Kij as a key to an opposite terminal device. Moreover, an encoder/decoder 107 encodes or decodes the data by using the **random** number **RN** as a key. Thus, the output of the scrambler 106 and the encoder/ decoder 107 is obtained externally.

12/5/6 **(Item 6 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014190773 **Image available**
WPI Acc No: 2002-011470/200201
XRPX Acc No: N02-009486
Encryption **using transparent keys e.g. for** encrypting **and decrypting electronic mail which minimizes likelihood of key management problems**
Patent Assignee: VU K Q (VUKQ-I)
Inventor: VU K Q
Number of Countries: 095 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200184766	A2	20011108	WO 2001US13443	A	20010427	200201 B
AU 200157296	A	20011112	AU 200157296	A	20010427	200222
US 6640303	B1	20031028	US 2000200272	P	20000428	200372
			US 2000667607	A	20000922	

Priority Applications (No Type Date): US 2000667607 A 20000922; US 2000200272 P 20000428
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200184766	A2	E	38	H04L-009/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200157296	A		H04L-009/00	Based on patent WO 200184766
US 6640303	B1		H04L-009/08	Provisional application US 2000200272

Abstract (Basic): WO 200184766 A2

NOVELTY - Each party has a secret, unique, **randomly** assigned value y. The **sender** and **receiver** engage in a handshake, and the **sending** party is given the y value of the **receiving** party. A key is then generated **randomly** and used by the **sending** party to **encrypt** a byte of information to be sent.

DETAILED DESCRIPTION - A **new key** is generated for every byte to be **encrypted** . The resulting **ciphertext** is a combination of the output of a function F and a function P. F is a function of plaintext and the key. P is a function of the plain text and the y value of the **receiving** party. The y values and keys are not readily apparent to users. An INDEPENDENT CLAIM is included for a system and a computer program product.

USE - For **encrypting** and decrypting information e.g. electronic mail.

ADVANTAGE - Minimizes likelihood of key management problems e.g. loss or compromise of keys.

DESCRIPTION OF DRAWING(S) - The drawing shows a flow diagram of the method.

pp; 38 DwgNo 1/16

Title Terms: **ENCRYPTION** ; TRANSPARENT; KEY; ELECTRONIC; MAIL; MINIMISE; KEY; MANAGEMENT; PROBLEM
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/00** ; **H04L-009/08**
International Patent Class (Additional): **H04K-001/02** ; **H04L-009/16**
File Segment: EPI

12/5/7 **(Item 7 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012990918 **Image available**
WPI Acc No: 2000-162770/200015
XRPX Acc No: N00-121544
Information processing method for processing information on an encryption basis for digital recording media eg. Digital versatile disc
Patent Assignee: VICTOR CO OF JAPAN (VICO)
Inventor: YOKOUCHI K
Number of Countries: 026 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 977107	A2	20000202	EP 99113424	A	19990712	200015	B
JP 2000048483	A	20000218	JP 98230011	A	19980731	200020	

Priority Applications (No Type Date): JP 98230011 A 19980731
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 977107	A2	E	33	G06F-001/00	
JP 2000048483	A		10	G11B-020/10	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 977107 A2

NOVELTY - A data processing unit (41) stores and retrieves an intermediate key, in response to an identifier **transmitted** from an audio or video reproduction device, and decides whether or not the retrieved intermediate **key** and a **second** intermediate **key** are equal to each other.

DETAILED DESCRIPTION - A data processing apparatus (41) generates an intermediate key in response to a **random** number key, and stores the intermediate key in connection with an identifier. A combination of the identifier and the **random** number key is **transmitted** from the data processing device to an audio or video reproduction device which generates a **second** intermediate **key** in response to the **random** number key. A combination of the identifier and the **second** intermediate **key** is **transmitted** from the reproduction device to the data processing device. The processing unit (41) also retrieves the first intermediate key in response to the identifier **transmitted** from the reproducing device, and decides whether or not the retrieved first intermediate **key** and the **second** intermediate **key** are equal to each other. INDEPENDENT CLAIMS are included for; a system for processing information;

USE - Processing information on an **encryption** basis in recording media storing digital information eg. Audio and video data stored on CD or DVD.

ADVANTAGE - Enables data processing apparatus to **encrypt** and decrypt digital information **transmitted** between audio/video reproduction device, and data processor.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of an information processing system according to a first embodiment of the invention.

Digital storage medium (11)
Recording medium drive device (21)
Data bus (31)
Data processing apparatus (41)
pp; 33 DwgNo 1/13

Title Terms: INFORMATION; PROCESS; METHOD; PROCESS; INFORMATION; **ENCRYPTION** ; BASIS; DIGITAL; RECORD; MEDIUM; DIGITAL; VERSATILE; DISC
Derwent Class: T01
International Patent Class (Main): **G06F-001/00** ; G11B-020/10
International Patent Class (Additional): G09C-001/00; **H04L-009/08** ; **H04L-009/32**
File Segment: EPI

EP 718803	A2	19960626	EP 95120424	A	19951222	199630	B
CA 2165102	A	19960623	CA 2165102	A	19951213	199642	
JP 8273011	A	19961018	JP 95333683	A	19951221	199701	
US 5606613	A	19970225	US 94361409	A	19941222	199714	
CN 1131851	A	19960925	CN 95121346	A	19951222	199801	
CA 2165102	C	20021210	CA 2165102	A	19951213	200305	

Priority Applications (No Type Date): US 94361409 A 19941222
Cited Patents: No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 718803	A2	E	8	G07B-017/04	
Designated States (Regional): DE FR GB					
CA 2165102	A			G07B-017/02	
JP 8273011	A		7	G07B-017/00	
US 5606613	A		6	H04L-009/00	
CN 1131851	A			H04L-009/00	
CA 2165102	C	E		G07B-017/02	

Abstract (Basic): EP 718803 A

The method **encrypts** and decrypts data using an **encryption** key, and operates a digital printer (21) to **encrypt** or decrypt the postage data using the key. A **random** number is generated, which is **encrypted** at the printer, and **transmitted** to the meter (11) after **encryption**.

The **random** number is decrypted and re- **encrypted** in such a way to have a known relationship to the original **random** number. The re- **encrypted** **random** number is **transmitted** together with the known relationship to the printer. The re- **encrypted** **random** number is decrypted with the known relationship and the relationship is verified. The digital printer is enabled upon verification.

USE/ADVANTAGE - Relates to postage metering system with postage accounting system remotely located to postage printer. Prints postage indicia unless digital printer is in electronic communication with specific vault system.

Dwg.1/2

Title Terms: VERIFICATION; SPECIFIC; OPERATE; COMBINATION; POSTAGE; METER; CONTROL; GENERATE; **RANDOM** ; NUMBER; **TRANSMIT** ; METER; RELATED; ORIGINAL ; **TRANSMIT** ; PRINT; NUMBER; RELATED; ENABLE; PRINT
Derwent Class: P75; P85; T04; T05; W01
International Patent Class (Main): G07B-017/00; G07B-017/02; G07B-017/04; **H04L-009/00**
International Patent Class (Additional): B41J-005/30; B41J-029/38; G09C-001/00; **H04L-009/10**
File Segment: EPI; EngPI

12/5/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010277213 **Image available**
WPI Acc No: 1995-178468/199523
XRPX Acc No: N95-140175
Encrypted **data transmission system contg facility for** randomly **alteration** encryption **keys - uses key memory which permits unique serial number identifying remote unit to be stored along with current** encryption **key value**
Patent Assignee: TELEQUIP CORP (TELE-N)
Inventor: JONES M F
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5412730	A	19950502	US 89418178	A	19891006	199523	B
			US 92872674	A	19920423		

Priority Applications (No Type Date): US 92872674 A 19920423; US 89418178 A 19891006

12/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011079309 **Image available**
WPI Acc No: 1997-057233/199706
XRPX Acc No: N97-047107
Client authentication system for digital audio interactive system - includes comparator that compares enciphered **data from MASC and authentication part based on which it is judged that client has performed access demand**
Patent Assignee: FUJITSU LTD (FUIT)
Inventor: AKIYAMA R; ISHIZAKI M; KOGA Y; MUNAKATA A
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8305662	A	19961122	JP 95108408	A	19950502	199706	B
US 5784464	A	19980721	US 96594895	A	19960131	199836	

Priority Applications (No Type Date): JP 95108408 A 19950502
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8305662	A		22	G06F-015/00	
US 5784464	A			H04L-009/00	

Abstract (Basic): JP 8305662 A

The system includes a service donor side system which has a key management part (18). A service client (6) is connected to a MASC (5). When the client performs an access demand, the key management part forms an individual key (K) which is then **transmitted** to an authentication part (15). The individual key is also stored in the MASC beforehand. A **random** number generator (20) generates **random** number (R) which is **transmitted** to MASC and authentication part.

MASC **enciphers** the **random** number with the individual key and the first **enciphered** data is **transmitted** to the donor side system by a **transmitting** unit. An **encipherment** part (151) of the authentication part **enciphers** the **random** number with the individual **key** to obtain **second enciphered** data. A comparator (152) compares the two **enciphered** data. When they are equal, it is judged that the client has performed access demand.

ADVANTAGE - Produces recognition information used in authentication dynamically. Prevents surreptitious use by third person. Enables service donor to collect price reliably.

Dwg.6/14

Title Terms: CLIENT; AUTHENTICITY; SYSTEM; DIGITAL; AUDIO; INTERACT; SYSTEM ; COMPARATOR; COMPARE; **ENCIPHER** ; DATA; AUTHENTICITY; PART; BASED; JUDGEMENT; CLIENT; PERFORMANCE; ACCESS; DEMAND
Derwent Class: T01
International Patent Class (Main): **G06F-015/00 ; H04L-009/00**
International Patent Class (Additional): **G06F-013/00 ; H04K-001/00**
File Segment: EPI

12/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010792189 **Image available**
WPI Acc No: 1996-289142/199630
Verifying specific operable combination of postage metering controller - generates and encrypts random **number and** transmits **it to meter, decrypts and re-** encrypts **with known relationship to original and** transmits **to printer, where number and relationship is decrypted to enable printer**
Patent Assignee: PITNEY BOWES INC (PITB)
Inventor: LEE Y W; MOH S; MULLER A
Number of Countries: 007 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

```
Set     Items   Description
S1     221970   KEY OR KEYS OR KEYPAIR?
S2     231752   RANDOM? OR PSEUDORANDOM? OR SEED? OR PEARL? OR RN
S3     752873   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR PROTECT? OR CYPHER? -
             OR CIPHER?
S4    2698284   TRANSMIT? OR SEND? OR DELIVER? OR RECEIV?
S5       4999   S1(2N)(SECOND OR 2ND OR ADDITIONAL OR NEW OR SINGLE()USE? -
             OR DISPOSABLE?)
S6     774095   TEXT? OR MESSAG?
S7        109   S2 AND S3 AND S4 AND S5
S8        105   S7 AND IC=(G06F? OR H04N? OR H04K? OR H04L?)
S9       6754   S2(4N)S4
S10        34   S8 AND S9
S11        34   IDPAT (sorted in duplicate/non-duplicate order)
S12        34   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2004/Apr(Updated 040802)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200452
         (c) 2004  Thomson Derwent
?
```

```
Set     Items   Description
S1     221970   KEY OR KEYS OR KEYPAIR?
S2     231752   RANDOM? OR PSEUDORANDOM? OR SEED? OR PEARL? OR RN
S3     752873   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR PROTECT? OR CYPHER? -
             OR CIPHER?
S4    2698284   TRANSMIT? OR SEND? OR DELIVER? OR RECEIV?
S5       4999   S1(2N)(SECOND OR 2ND OR ADDITIONAL OR NEW OR SINGLE()USE? -
             OR DISPOSABLE?)
S6     774095   TEXT? OR MESSAG?
S7        109   S2 AND S3 AND S4 AND S5
S8        105   S7 AND IC=(G06F? OR H04N? OR H04K? OR H04L?)
S9       6754   S2(4N)S4
S10        34   S8 AND S9
S11        34   IDPAT (sorted in duplicate/non-duplicate order)
S12        34   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2004/Apr(Updated 040802)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200452
         (c) 2004  Thomson Derwent
?
```

12/5/1 **(Item 1 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

016182012 **Image available**
WPI Acc No: 2004-339899/200431
Related WPI Acc No: 2004-315016; 2004-355439
XRPX Acc No: N04-271773

Computing device authentication method for wireless-fidelity network, involves transmitting task with random number encrypted by secret cryptographic key, to computing device

Patent Assignee: FASCENDA A C (FASC-I); VARIAN INC (VARI-)
Inventor: FASCENDA A C; SHEEHAN T L
Number of Countries: 030 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20040073797	A1	20040415	US 2002416583	P	20021008	200431 B
			US 2002422465	P	20021030	
			US 2002422474	P	20021031	
			US 2003447921	P	20030219	
			US 2003679371	A	20031007	
WO 200442384	A1	20040521	WO 2003US34442	A	20031029	200434

Priority Applications (No Type Date): US 2003679371 A 20031007; US 2002416583 P 20021008; US 2002422465 P 20021030; US 2002422474 P 20021031; US 2003447921 P 20030219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040073797	A1		25	H04L-009/00	Provisional application US 2002416583
					Provisional application US 2002422465
					Provisional application US 2002422474
					Provisional application US 2003447921
WO 200442384	A1	E		G01N-030/72	

Designated States (National): AU CA JP US
Designated States (Regional): AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR

Abstract (Basic): US 20040073797 A1

NOVELTY - A task is **received** from one of the computing devices (210A-210N), that has **encrypted random** number and serial number of physical token related with computing device. A secret cryptographic key related to token is obtained, and another **random** number is generated. The **random** numbers are decrypted/ **encrypted** with key, respectively. Another task having **encrypted random** number, is **transmitted** to device.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) method of deriving **new encryption key** for communication session; and

(2) communication system.

USE - For authenticating computing devices like personal digital assistant (PDA), desktop computer in wireless-fidelity (Wi-Fi) network.

ADVANTAGE - Since authentication and security solution are implemented in the access point, the need for additional network appliances or server software is eliminated, thereby the cost is reduced and less maintenance is required. The secure communication and authentication are difficult to hack by an interloper, by using minimal number of cryptographic keys. Enables providing unique identification of each user, transparent roaming, and positive authentication without the use of back-end servers. Reduces the time and cost to deploy secured Wi-Fi networks, and simplifies network operation.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic diagram of the Wi-Fi communication system.

Wi-Fi network (200)
wireless access point (220)
master key (230)

client keys (240A-240N)
access point key (250)
pp; 25 DwgNo 2/12

Title Terms: COMPUTATION; DEVICE; AUTHENTICITY; METHOD; WIRELESS; FIDELITY; NETWORK; **TRANSMIT** ; TASK; **RANDOM** ; NUMBER; **ENCRYPTION** ; SECRET; CRYPTOGRAPHIC; KEY; COMPUTATION; DEVICE

Derwent Class: T01; W01

International Patent Class (Main): G01N-030/72; **H04L-009/00**

International Patent Class (Additional): B01D-015/08

File Segment: EPI

12/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015113927 **Image available**
WPI Acc No: 2003-174447/200317
XRPX Acc No: N03-137352

Block organized data transmission method in symmetric key encryption **system, involves generating** new encryption key **at both** sender **and** receiver , **by pseudo** random **functional unit**

Patent Assignee: KEYGEN CORP (KEYG-N)
Inventor: RANDALL D L; RUBINSTEIN I I
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020159598	A1	20021031	US 9763919	P	19971031	200317 B
			US 98182154	A	19981029	
			US 2000254460	P	20001208	
			US 200121268	A	20011207	

Priority Applications (No Type Date): US 200121268 A 20011207; US 9763919 P 19971031; US 98182154 A 19981029; US 2000254460 P 20001208
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020159598	A1		19	H04L-009/00	Provisional application US 9763919
					CIP of application US 98182154
					Provisional application US 2000254460

Abstract (Basic): US 20020159598 A1

NOVELTY - An initialization string is exchanged between a **sender** and a **receiver** . An **encryption** key is generated using data including initialization string at both **sender** and **receiver** . The next block of data is **encrypted** into **ciphertext** by symmetric key **encryption** algorithm, and **ciphertext** is decrypted. A **new encryption key** is generated at both **sender** and **receiver** by a pseudo **random** functional unit.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for **encryption** key generation and updating method.

USE - For **transmitting** block organized data in symmetric key **encryption** system.

ADVANTAGE - The **encryption** system is able to discern the difference between transmission error and an attempt at intrusion, and to take steps accordingly.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart explaining the block organized data transmission method.

pp; 19 DwgNo 1/7

Title Terms: BLOCK; ORGANISE; DATA; TRANSMISSION; METHOD; SYMMETRICAL; KEY; **ENCRYPTION** ; SYSTEM; GENERATE; NEW; **ENCRYPTION** ; KEY; **SEND** ; **RECEIVE** ; PSEUDO; **RANDOM** ; FUNCTION; UNIT
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/00**
File Segment: EPI

12/5/8 **(Item 8 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

012652669 **Image available**
WPI Acc No: 1999-458774/199938
XRPX Acc No: N99-343172
Cellular-phone-unique- encryption **key dynamic updating method for cellular phone network**
Patent Assignee: DSC TELECOM LP (DSCT-N)
Inventor: MILLS K M
Number of Countries: 022 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9938288	A1	19990729	WO 99US2066	A	19990127	199938	B
US 5991405	A	19991123	US 9814121	A	19980127	200002	
EP 1051820	A1	20001115	EP 99905566	A	19990127	200059	
			WO 99US2066	A	19990127		
CN 1291390	A	20010411	CN 99803224	A	19990127	200140	

Priority Applications (No Type Date): US 9814121 A 19980127
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9938288	A1	E	32	H04L-009/16	
Designated States (National): CN JP KR					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
US 5991405	A			H04L-009/32	
EP 1051820	A1	E		H04L-009/16	Based on patent WO 9938288
Designated States (Regional): DE ES FR GB IT SE					
CN 1291390	A			H04L-009/16	

Abstract (Basic): WO 9938288 A1
NOVELTY - A **new** , common **encryption key** is calculated independently in the cellular phone (1) and an associated home location register (HLR) (2), one of which by means of a number-manipulating algorithm using a shared secret **random** data (102) and the prestored **encryption** key, while the other by means of another number-manipulating algorithm using an independently calculated **random** data and the **encryption** key.
DETAILED DESCRIPTION - The shared secret **random** data is calculated in either the phone or HLR by means of another number-manipulating algorithm using a **random** number (101) and the **encryption** key. A message including the **random** number and **random** data is **transmitted** from the phone or HLR, where the **random** data are calculated, to the other. The **random** data is calculated in the other, independently of the first calculation, by means of another number-manipulating algorithm using the **random** number and **encryption** key.
USE - For cellular phone network.
ADVANTAGE - Prevents fraudulent use of cellular phones since the **new encryption key** independently calculated by cellular phone and HLR is not **transmitted** during updating process, thereby eliminating possibility of **new encryption key** being intercepted by unauthorized parties during transmission. Does not require transmission of updated **encryption** keys between cellular phone and associated central processing facility or HLR for verification. Requires no protocol change in existing cellular telephone network.
DESCRIPTION OF DRAWING(S) - The drawing shows the transmission of data messages between the HLR and cellular phone which occurs in the dynamic update process initiated by the HLR.
Cellular phone (1)
Home location register (2)
Random number (101)
Shared secret **random** data (102)
pp; 32 DwgNo 1/2
Title Terms: CELLULAR; TELEPHONE; UNIQUE; **ENCRYPTION** ; KEY; DYNAMIC; UPDATE; METHOD; CELLULAR; TELEPHONE; NETWORK

Derwent Class: W01
International Patent Class (Main): **H04L-009/16 ; H04L-009/32**
International Patent Class (Additional): **H04L-009/28**
File Segment: EPI

```
Set     Items   Description
S1    1352850   KEY OR KEYS OR KEYPAIR?
S2    1911706   RANDOM? OR PSEUDORANDOM? OR SEED? OR PEARL? OR RN
S3    1903512   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR PROTECT? OR CYPHER? -
            OR CIPHER?
S4    3655846   TRANSMIT? OR SEND? OR DELIVER? OR RECEIV?
S5      23327   S1(2N)(SECOND OR 2ND OR ADDITIONAL OR NEW OR SINGLE()USE? -
            OR DISPOSABLE?)
S6    1814887   TEXT? OR MESSAG?
S7        198   S2 AND S3 AND S4 AND S5
S8        146   (S6 OR CYPHERTEXT) AND S7
S9        198   S2(4N)S2 AND S7
S10   1911706   S2(2N)S2
S11       146   S8 AND S10
S12       135   RD (unique items)
S13       117   S12 NOT PY>2001
S14       108   S13 NOT PD>20010116
S15      7225   S1(2N)S4
S16        28   S14 AND S15
S17        28   S2(3N)S5
S18        28   S17 NOT S16
S19        21   RD (unique items)
S20        18   S19 NOT PY>2001
S21        18   S20 NOT PD>20010116
S22     38736   S2(2N)(NUMBER? OR STRING?)
S23        38   S7 AND S22
S24        27   S23 NOT (S16 OR S21)
S25        27   RD (unique items)
S26        20   S25 NOT PY>2001
S27         2   S15 AND S26
File   8:Ei Compendex(R). 1970-2004/Aug W2
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/May
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Jul 12
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Aug W2
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Aug W2
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Jul W4
         (c)2004 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Aug 11
         (c) 2004 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File   6:NTIS 1964-2004/Aug W3
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Aug W2
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Aug W2
         (c) 2004 Inst for Sci Info
File  62:SPIN(R) 1975-2004/Jun W3
         (c) 2004 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Jul
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Jun W1
         (c) 2004 FIZ TECHNIK
File 239:Mathsci 1940-2004/Oct
         (c) 2004 American Mathematical Society
File 636:Gale Group Newsletter DB(TM) 1987-2004/Aug 16
         (c) 2004 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Aug 16
         (c) 2004 The Gale Group
File 647:CMP  Computer Fulltext 1988-2004/Aug W1
         (c) 2004 CMP Media, LLC
```

16/5/15 **(Item 10 from file: 275)**
DIALOG(R)File 275:Gale Group Computer DB(TM)

01891305 SUPPLIER NUMBER: 17990734 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The DCE security service. (the security protocol in the Open Software Foundation's Distributed Computing Environment specification) (includes glossary) (Technology Information)
Gittler, Frederic; Hopkins, Anne C.
Hewlett-Packard Journal, v46, n6, p41(8)
Dec, 1995
ISSN: 0018-1153 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 6029 LINE COUNT: 00487

ABSTRACT: The security services of the Open Software Foundation's Distributed Computing Environment (DCE) enables the secure transmission of data between two parties in a DCE-based client/server environment. DCE is a standard specification for integrated services supporting distributed applications in heterogeneous client/server computing and network environments. The DCE security service combines the Kerberos version 5 **encryption** and authentication system with other tools to identify and authenticate users, enable applications to decide on whether to allow access, and secure data communications. The architecture and implementation of a DCE security service; the use of a central registry database containing the user and account passwords, keys and identifiers; extended registry attributes; and security system requirements are discussed.

SPECIAL FEATURES: illustration; chart
DESCRIPTORS: Technology Overview; Systems/Data Security Software; Standard
FILE SEGMENT: CD File 275

16/5/20 **(Item 15 from file: 275)**
DIALOG(R)File 275:Gale Group Computer DB(TM)

01690848 SUPPLIER NUMBER: 15562797 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Confidentially speaking. (E-mail security) (Cover Story)
Stallings, William
LAN Magazine, v9, n8, p49(4)
August, 1994
DOCUMENT TYPE: Cover Story ISSN: 0898-0012 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3186 LINE COUNT: 00252

ABSTRACT: The Internet Engineering Task Force's Privacy Enhanced Mail (PEM) security standard has been adopted by a wide variety of E-mail applications for platforms such as Unix, DOS and Macintosh. An E-mail **message** that is processed by PEM-enabled applications is converted to a canonical form that makes it interoperable among different systems. The **message** is then processed through integrity and authentication schemes. The standard uses the RSA public-key **encryption** algorithm and the MD5 one-way hash function to create digital signatures. PEM **encrypts messages** in the third step. **Senders** use the data **encryption** standard (DES) to create **single - use** data **encryption keys** (DEK). DES is a type of symmetric **encryption** technology that requires **senders** and **receivers** to know the secret key in order to lock and unlock **messages** .
SPECIAL FEATURES: illustration; table; chart
DESCRIPTORS: E-Mail; Privacy; Data Integrity; Software Design; **Encryption** ; Standard
SIC CODES: 4822 Telegraph & other communications
FILE SEGMENT: CD File 275

16/5/23 **(Item 18 from file: 275)**
DIALOG(R)File 275:Gale Group Computer DB(TM)

01602214 SUPPLIER NUMBER: 13924423 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Cryptography: breaking the code. (an encryption **program that uses a** random **number generator) (Column) (What's the Code?) (Tutorial)**
Stafford, David
Computer Shopper, v13, n7, p558(2)
July, 1993
DOCUMENT TYPE: Tutorial ISSN: 0886-0556 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1816 LINE COUNT: 00135

ABSTRACT: A method of creating a secure **encryption** code using a pseudo-**random** number generator is presented. The resulting **encryption** is so secure that it is almost impossible to break it, unless code analyzers know the **encryption** algorithm. However, even if the analyzers know the algorithm, they still have to select among 4,294,967,296 choices to locate the 32-bit key. The innovation behind the **encryption** program is to use the **seed** that generates **random** numbers as the key to the **encryption** code. The program includes the main() function, which ensures that the program contains four parameters; the supervisor() function, which opens files and provides error **messages** ; the **cipher** () function, which encodes the input; and the GetRandomNumber() function, which generates pseudo-**random** numbers.

SPECIAL FEATURES: illustration; program
DESCRIPTORS: **Encryption** ; Code Breaking; Cryptography; Pseudo- **Random** Number Generation; Program Development Techniques; Tutorial; Data Security
FILE SEGMENT: CD File 275

16/3,K/28 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01185073 CMP ACCESSION NUMBER: INW19990215S0047

Maintaining PKI's Sterile Environment

Rutrell Yasin

INTERNETWEEK, 1999, n 752, PG27
PUBLICATION DATE: 990215
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Management & Security
WORD COUNT: 410

... on the Internet. By generating a public/private key pair, a person or company can **encrypt** a confidential **message** using a private **key** and **send** it using a public key. The public key can be opened only by the intended...

...user can compute a dirty key pair to map an existing signature onto a new **message** , substituting one **message** for another. Users can also spoof or alter a key agreement scheme by setting a...

...Authority, which binds a person's or company's identity to a digital certificate, insert **random** data into a user's public key to prevent the key from being exploited. The CA would then **send** the clean **key** with a certificate back to the user, who would then compute a **new** private **key** based on the information inserted by the CA.

While none of the dirty key exploits...

21/5,K/6 **(Item 1 from file: 233)**
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00501425 98BY07-005

S/MIME: e-mail gets secure -- This proposed standard protects your Internet e-mail from eavesdroppers and tampering

Stallings, William

BYTE , July 1, 1998 , v23 n7 p41-42, 2 Page(s)
ISSN: 0360-5280
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States

Spotlights Secure Multipurpose Internet Mail Extensions (S/MIME). Defines it as a security enhancement to the MIME Internet-based e-mail format standard and claims that it is bound to become the industry standard for commercial use. Notes, however, that it will not replace PGP as the personal e-mail security standard. Lists, and explains, the four new content functions of S/MIME: enveloped data, signed data, clear-signed data, and signed and enveloped data. Says that it provides enhanced security by **randomly** generating a **new key** for every message, attaching the key to the message when it is sent. Also notes the relationship between S/MIME and public-key certificates in which the holder of the key, or user ID, ``signs'' a transmission to attest to its validity. Claims that though S/MIME is not so widely implemented at present, all users will eventually rely on some sort of public-key infrastructure. Includes one diagram and one table. (kgh)

Descriptors: Security; Standards; Electronic Mail; Internet; Messaging; Networks; Privacy

... clear-signed data, and signed and enveloped data. Says that it provides enhanced security by **randomly** generating a **new key** for every message, attaching the key to the message when it is sent. Also notes...

21/5,K/17 **(Item 3 from file: 647)**
DIALOG(R)File 647:CMP Computer Fulltext

01076695 CMP ACCESSION NUMBER: EET19951211S0095

V-One raises SmartGate

Brian Santo

ELECTRONIC ENGINEERING TIMES, 1995, n 879, PG106
PUBLICATION DATE: 951211
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: The Profession - Interactive Engineering
WORD COUNT: 553

TEXT:

Rockville, Md. - The Virtual Open Network Environment Corp. (V-One) today will introduce SmartGate, a client/server application that can be dropped in as a secure gateway on most network servers. SmartGate ensures mutual authentication by client and server, thereby providing a higher network security than firewalls or other secure-server technologies, the company said.

... s identities and, rather than generate a new public key just for the session, a **new random key** is generated. Either the DES or RC4 algorithm is employed.

Secure identification data and encryption...

27/5,K/2 **(Item 1 from file: 647)**
DIALOG(R)File 647:CMP Computer Fulltext

00607536 CMP ACCESSION NUMBER: NWC19910701S2952
Network Security Seeking Security in the Enterprise-wide Network (Feature 1)
Timothy Haight
NETWORK COMPUTING, 1991, n 207 , 50
PUBLICATION DATE: 910701
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Features
WORD COUNT: 3374
TEXT:

Protecting a mainframe or minicomputer means guarding one big box that's locked behind the doors of the "glass house." The computer has only one operating system with several effective security features. These include extensive audit trails and isolation of the security software from the rest of the system. In short, physical access to the computer is controlled, and logical access through its ports is guarded by the operating system.

TEXT:

Protecting a mainframe or minicomputer means guarding one big box that's locked behind the doors...

... and potentially weak links abound. Figure 1 shows 15 points in a network where password **protection** can be compromised.

Most computer crimes are committed by authorized users. But more users each...

...of password changes; it can waste your time as you wait for your PC to **encrypt** a huge file. Security may mean losing access to a workmate's PC after hours if his or her disks are password **protected** . And, if people only hear about security breaches in the newspapers, they may take the...

...low-cost software-only "sniffers" is posing a new threat.

Although some LAN operating systems **protect** passwords by **encryption** or with challenge-response mechanisms (which are discussed later), others are vulnerable, as are some...

...be tapped using the right equipment stuffed in a car that's parked behind the **receiving** dish.

As the chances to snare a password grow, so does the number of passwords...

...systems. But until the days of unencrypted and unchanging passwords end, networks are at risk.

Encryption can foil tapping, and effective systems for **encryption** are available. But even this approach has limits. Packets **encrypted** at a workstation may have to be decoded at each router for the routing information...

...a point of clear-text access. Routers may also need to be updated whenever an **encryption** key is changed, which is an inconvenience.

Further along the network ...workstation on a LAN take control of another.

While access can be turned off or **protected** by a password, usually lacking are such features as an auditing facility that records repeated...

...for details) information security managers are following four general trends: observing the fundamentals, educating users, **encrypting** data and employing dynamic one-time authentication.

Observing the fundamentals means setting up and maintaining... conduits that set off alarms if penetrated. But a network can quickly extend beyond the **protection** of such physical security measures. And with key information outside the control of operating systems...

...secure operating system has its limits. As a result, security practices are increasingly turning to **encryption** .

Effective **encryption** can combat such security breaches as wiretapping or unauthorized file access. The problem is building an **encryption** system that encodes and decodes messages easily for authorized users without yielding to unauthorized users...

...their keys are secret, be secure. An example of such an algorithm is the Data **Encryption** Standard (DES) developed by the National Institute of Standards and Technology (NIST). Products based on...

...What's more, the algorithm is easy to use because it can be built into **encryption** programs and then combined with a secret key to produce effective **encryption** .

Encryption systems can be symmetric or asymmetric. In a symmetric system, the **sender** and **receiver** use the same algorithm and key. Such a system requires that all the **senders** and **receivers** be trustworthy, and that they all be able to keep their keys secret. Because someone can break into an unprotected system and discover the **encryption** key, it is also necessary to change the key periodically. Changing the key requires redistributing...

...of key management hinting at some of its difficulties is that keys should never be **transmitted** over the same communications channel as the material they are used to **encrypt** .

Key management is easier in an asymmetric **encryption** system, where different keys serve for encoding and decoding. In this method, someone distributes an...

...on the same network have their own private decoding keys and only distribute their public **encryption** key. Thus, instead of having one key that decodes all the messages on the network...

...anybody else. Consequently, only the private keys require secrecy, which simplifies their management.

Public-key **encryption** , where every person has his or her own personal key, also solves the security problem...

...person authorized to make it. With a public key crypto-system, authentication happens when the **sender** **encrypts** a message twice. First, the **receiver** 's public **key** provides the basis for an **encryption** . Then the **sender** 's private **key** **encrypts** the message again. The **receiver** uses his or her private key to decode the **sender** 's public **key** **encryption** , then uses the **sender** 's public **key** to verify that it came from the right person. Other methods of authentication distribute an authentication key and algorithm unrelated to the message **encryption** process.

Unfortunately,the inherent contradiction between security and communication inhibits the advance of **encryption** technology. Usually, when complicated technologies are evaluated for effectiveness, the methods of evaluation are made...

...have been widely discussed and became de facto standards as a result.

But examining an **encryption** system this way could compromise its effectiveness. Thus, certain cryptography research has been classified. Beyond DES and RSA it is difficult to assess the quality of an **encryption** system either because those who know won't say or those who would say or ...

...much of America's computer industry sells overseas, export limits are a disincentive to building **encryption** into general purpose products. Security tends to be relegated to special-purpose products, a practice that further limits their sales.

These complex relationships tend to limit the supply of **encryption** systems, limit incentive to develop new ones and lead to systems that are costly making...

...patented, which adds license fees to the costs of products that use it.

Public-key **encryption** systems also sap substantial computing power, limiting **encrypted** data rates to only a few Kbps of throughput. In contrast, private-key systems like DES can **encrypt** at rates up to 45 Mbps, with even higher **encryption** rates expected soon. On the other hand, key management with DES is more of a problem.

For most organizations, an **encryption** system based on the DES if the effort is made to use it properly will...

...the resources necessary to decode it without being given the key are very high. But **encryption** technology is still a work-in-progress. New algorithms from NIST are expected. But there...

...Fixed passwords, which are subject to tapping and other compromises , can be also secured by **encryption** . Methods range from simple private -key **encryption** between workstation and server to more complicated methods such as Kerberos, an authentication system developed...

...Computing environment.

Challenge-response techniques are effective for authentication, in part because they do not **send** passwords from the user to the authenticating computer. Instead, the user **sends** his or her user name. The computer has a key for the user, which is used to **send** a number some function of the key and a **random number** back to the user. The user, who also has the key, decodes the number, then...

...end has. When the computer decodes the number sent back by the user with the **second key** and sees the original **random number** , it knows the user is authentic.

The problem, of course, is that this requires the...

?ds;hsow files